UOT 327: 140.8

Nurəddin MEHDİYEV
Azərbaycan Respublikasının Prezidenti yanında
Dövlət İdarəçilik Akademiyası, dissertant
nuraddin_mehdiyev@yahoo.com

BEYNƏLXALQ İNFORMASİYA MÜHARİBƏLƏRİNDƏ İKT AMİLİ

Xülasə

İKT-nin inkişafı dünyada böyük dəyişikliklərə səbəb olmuşdur. Son dövrdə beynəlxalq terrorizm, müxtəlif xarakterli transmilli qurumlar internet imkanlarından istifadə edərək öz təsir dairəsini daha da genişləndirirlər. Onlar çox vaxt ölkələr arasında qarşıdurma yaratmaq üçün internet vasitəsilə süni təxribatlar yaradırlar. Bəzi hallarda bunlar ölkələr arasında narazılığın yaranmasına və müəyyən müqavilələrin pozulmasına şərait yaradır. İnformasiya müharibələrində istifadə olunan informasiya silahları informasiya məkanında olan dövlət qurumlarının təhlükəsizliyini təhdid edir. Çünki milli hökumətlər informasiya məkanına tam nəzarət edə bilmirlər. Nəticədə, milli suverenitetin təminatının və beynəlxalq münasibətlərin təhlükəsizliyinin ənənəvi konsepsiyaları öz aktuallığını itirir.

Məqsəd: beynəlxalq informasiya müharibələrinin xarakterini, mahiyyətini, beynəlxalq münasibətlər sisteminə təsirini və onun nəticələrini ortaya qoymaq, eyni zamanda, ondan qorunmağın yollarını müəyyənləşdirməkdir.

Metodologiya: məqalədə analiz, sintez, analogiya və müqayisəli təhlil metodlarından istifadə olunmuşdur.

Elmi yenilik: dünyada bir çox kibercinayətlərin ənənəvi beynəlxalq hüquq çərçivəsində həlli mümkün görünmür. Bu baxımdan İKT yeni beynəlxalq siyasət və hüquq konsepsiyalarının ortaya qoyulmasını zəruri edir.

Açar sözlər: qlobal informasiya, informasiya infrastrukturu, informasiya sistemi, İKT.

Giriş

"İnformasiya müharibəsi" (information war) rəsmi bir termin kimi, ABŞ-ın Müdafiə Nazirliyinin rəsmi sənədlərində istifadə olunmağa başlanmışdır. Pentaqon "hərbi idarəetmə sistemləri ilə müharibə doktrinası" adlı informasiya müharibəsi doktrinasını təsdiqlədikdən sonra, İKT-nin inkişafı ilə "informasiya müharibəsi" termini dünyada müxtəlif sahələri əhatə edən daha genişmənalı bir termin kimi istifadə olunmağa başladı.

İKT-nin inkişafı ənənəvi diplomatiya sistemini və dövlət idarəçiliyi institutlarını ortadan qaldırır. Buna görə də informasiya məkanı qlobal və regional güclərin toqquşma meydanına çevrilir. Toqquşmanın əsas tərəfləri qlobalistlər və antiqlobalistlərdir. Virtual məkanda monopoliyanı ələ alan qlobalistlər milli dövlətçilik və ənənəvi diplomatiya paradiqmalarından çıxış edən antiqlobalistləri kiberhücumlarla, trollinqlərlə müşayiət olunan informasiya müharibəsində məğlub etməyə çalışırlar.

Bu qarşıdurma özünü internetdə aşağıdakı kimi büruzə verir:

- təhlükəsizlik (dövlət xüsusi xidmət orqanları) və gizlilik (hüquq - müdafiə təşkilatları) tərəfdarları arasında qarşıdurma;
- dövlət süvereniteti və şəbəkə təşkilatları arasında toqquşma;
- açıq (open source) və qapalı proqram təminatı tərəfdarları (Microsoft) arasında qarşıdurma;
- müxtəlif xidmətlərin ödənişli və ödənişsiz olması ilə bağlı qarşıdurma;

- qanunvericilik və proqram tənzimlənməsi praktikasının toqquşması [1, s. 65].

M. Kastels internet kommunikasiyalar əsasında formalaşan sosial təşkilat və hərəkatların mahiyyətini aşağıdakı kimi səciyyələndirir [2, s. 44]:

- Sosial hərəkatlar təşkilati kimliyi formalaşdıran və paylaşılan mədəni dəyərlər ətrafında qurulmuşdur. İnternetdə müəyyən lokal və qlobal ideyalar ətrafında virtual qruplaşmalar meydana çıxır. Bu qruplar informasiya məkanında sosial kimlik formaları qazanaraq, virtual məkanda sosiallaşırlar. İnternet yeni cinayətlərin və beynəlxalq cinayətkarlar qrupunun formalaşmasına şərait yaradır. Virtual məkanda "çirkli pullar", narkotika, uşaq pornoqrafiyası, insan alveri, kardinq (kredit kartlarının kodlarının dağıdılması və yenilərinin hazırlanması) və digər cinayətlərin reallaşması üçün beynəlxalq cinayət əlaqələri yaradılır. Bu məkanda dövlətlər cinayətkarla təkbaşına mübarizə aparmaq imkanlarına malik deyildir. Onlara qarşı mübarizə qlobal səviyyədə mümkün olduğu üçün milli təhlükəsizliyin funksiyaları tədricən mexaniki şəkildə transmilli qurumların öhdəliyinə keçir. Bu isə, milli dövlətlərin əhəmiyyətini azaldır. Deməli, belə iddia etmək olar ki, beynəlxalq kibercinayətlərin arxasında dayanan güclər transmilli xarakterlidirlər.

- Onlar vətəndaş cəmiyyətinin ənənəvi siyasət qurumlarına (partiyalar, həmkarlar ittifaqları və rəsmi qeyri-hökumət təşkilatları) itən inamın yerini doldururlar. Dövlətlərin öz daxili siyasətində və beynəlxalq siyasətdə ədalət prinsipləri nə qədər çox pozulursa, bir o qədər fiziki-mənəvi zərər görmüş şəxslərin onlara etimadı azalır. Nəticədə, terror təşkilatları bundan istifadə edərək bu şəxslərin bir qismini öz ətrafında toplaya bilir.

- Onlar öz fəaliyyətlərinin qloballaşmasına çalışırlar. Çünki planetar genişlənmə lokal səviyyədə daha effektiv fəaiyyətə imkan verir. Məsələn, Əl-Qaidə, İŞİD (DAEŞ) kimi terror təşkilatları internet vasitəsilə özləri barədə mif yarada bilirlər. Onlara qarşı hərbi təzyiqlərin sayı artdıqca, onlar öz ətrafında tərəfdarlarının sayını artırmağa müvəffəq olurlar [8, s. 46].

Kibercinayətkarlığa qarşı mübarizə qlobal transmilli səviyyədə aparılır. İnformasiya müharibələrinin əsas meydanı sosial şəbəkələrdir. Orada müxtəlif akkauntlar arxasında gizlənən məhcul şəxs və ya qruplar şəbəkələri təlatümə gətirən şayiələr ortaya atır və sonra onların vasitəsilə minlərlə, milyonlarla insanların şüurlarını idarə etməyə başlayırlar. İnternetdə trollinq vasitəsilə etnik, dini, sosial və digər istiqamətlərdə ədavətlərin salınması, münaqişələrin yaradılması texnologiyası genişlənir [3]. Separatçı rejimlər, terrorçular və destruktiv qüvvələr kənardan İKT vasitəsilə dövlətlərin daxilində separatizm, terrorizm, ekstremizm və digər bu kimi təhlükəli amillərə əl atırlar. Bu baxımdan, İKT informasiya müharibələri üçün geniş şərait yaradır. Buna görə də üzv ölkələrin rəqəmsal diplomatiyanın neqativ təsirlərindən qorunması üçün informasiya sərhədlərinin təmin olunması məsələsi gündəmə gəlmişdir [4].

İnformasiya müharibəsi (kibernetik savaş) informasiyaya, düşmənin informasiya proseslərinə və informasiya sistemlərinə (strateji əhəmiyyətli siyasi, iqtisadi, sosial, hərbi və digər sahələrin obyektlərinə) informasiya silahı (kibernetik silah) ilə təsir etmək yolu ilə milli hərbi strategiyanı təmin etməkdə informasiya üstünlüyünə nail olmaq üçün alınan tədbirlərdən və dövlətin informasiyasını, informasiya proseslərini (informasiyanın əldə olunması, yaradılması, toplanması, işlənməsi, sistemləşdirilməsi, qorunması, aranması, yayılması, istifadəsi) və informasiya sistemlərini gücləndirib qorumaqdan ibarətdir [5**]**. Britaniyanın "The Economist" jurnalı informasiya müharibələrinin cərəyan etdiyi kiberməkanı müharibənin yer, dəniz, hava və kosmosdan sonra beşinci sahəsi olduğunu bildirmişdir [6, s. 45].

İnformasiya müharibəsinin silahı aşağıdakılardır:

- obyektin proqram təminatına müxtəlif növ səhvlərin yeridilməsi;
- məntiq bombaları (proqram əlamətləri);
- test proqramları vasitələrini neytrallaşdırmaq;
- kompüter virusları;

- telekommunikasiya şəbəkələrində informasiya mübadiləsinin dayandırılması;
- dövlət kanallarında və hərbi idarəetmədə məlumatların saxtalaşdırılması, dezinformasiyanın yayılması [8, s. 67].

Bir ölkənin digər ölkəyə qarşı apardığı informasiya müharibəsini informasiya təcavüzü, təcavüz edəni isə informasiya aqressoru kimi səciyyələndirirlər. İnformasiya aqressorunun tətbiq etdiyi informasiya silahı həm informasiya müharibəsinin xarakterini, həm də informasiya aqressorunun potensial imkanlarını müəyyənləşdirir. Kanada tədqiqatçısı M. Makluhan demişdir ki, "Üçüncü dünya müharibəsi – hərbiçilərlə mülki şəxslərin bir-birindən fərqlənmədiyi partizan informasiya müharibəsidir" [9, s. 20].

ABŞ və NATO hərbi təcavüzlərdən əvvəl informasiya müharibəsinin metodlarından səmərəli şəkildə istifadə edirlər. Çünki bu metodlar əksər hallarda hərbi qarşıdurma başlamadan əvvəl qələbə əldə etməyə və ya az itki ilə məqsədə nail olmağa imkan yaradır. ABŞ bu sahədə çox irəliyə getmişdir. 2010-cu ildə ABŞ kibernetik komandanlığının yaradılması, 2016-cı ildə ABŞ informasiya əməliyyatları qoşununun formalaşdırılması bunu təsdiq edir. ABŞ informasiya müharibəsinə ABŞ Dövlət Departamenti, ABŞ İnformasiya Agentliyi (USIA) və onun birləşmələri ("Amerikanın Səsi", "Azadlıq", "Azad Avropa"), MKİ (CIA) və Pentaqon psixoloqlarını cəlb edir. USIA materiallarının dünyanın müxtəlif informasiya agentliklərinə yayılması təmin edildiyi halda, onların ABŞ-da yayılması qadağan edilir [10, s. 62].

Rusiyanın siyasi-fəlsəfi təlimlər üzrə tanınmış tədqiqatçısı A. Duqin "Şəbəkə müharibələri: Yeni nəslin təhdidi" adlı əsərində yazır: "Əslində, Pentaqon strateqlərinin nəzərdə tutduğu şəbəkə sistemi ABŞ-ın bütün dünya üzərində qlobal üstünlüyünə xidmət edir, yəni, o, yeni şərtlər və vasitələrlə həyata keçirilən müstəmləkəçilik və itaətin postmodern analoqunu təşkil edir. Burada birbaşa işğala, çoxsaylı qoşunların yeridilməsinə və ya ərazilərin ələ keçirilməsinə, orduya və böyük hərbi xərclərə ehtiyac yoxdur. Şəbəkə - daha əlverişli silahdır. O, yalnız ekstremal hallarda şiddət və hərbi güc ilə manipulyasiya edir və əsas nəticələr informasiya, sosial, koqnitiv və digər amillərə təsir kontekstində əldə edilir. Burada aldanmaq olmaz: baş qərargahı məlum olmayan qlobal bir şəbəkə yaratmaqla, ABŞ öz maraqları çərçivəsində Amerika şəbəkəsi qurur. Qloballaşma bu maraqların ortaya çıxmasından qaynaqlanır. Lakin bu nə qədər səthi görünsə də, düşmənlərinə, dostlarına və neytral qüvvələrə qarşı şəbəkə müharibəsi aparan ABŞ-dır" [7, s. 26].

İnformasiya müharibəsinin əsas hədəfləri aşağıdakılardır:
- ölkənin siyasi və hərbi rəhbərliyi
- həyati önəm daşıyan sistemlər
- infrastrukturlar
- əhali
- müdafiə gücləri.

İnformasiya müharibəsi son strateji məqsədə çatana qədər düşmən ölkəyə qarşı davam etdirilən daimi müharibədir. Onun son mərhələsi hərbi təcavüz və ölkənin strateji obyektlərinin nəzarət altına alınması ilə bitə bilər. Əksər hallarda, bunlara hərbi təcavüz etmədən də nail olmaq olar. Məhz informasiya müharibəsi silahları buna şərait yaradır [11, s. 104].

İnformasiya müharibəsi öz hədəf və vəzifələrinə görə kibercəsusluq və təcavüz kateqoriyalarına bölünür.

1. Kibercəsusluq - zərərli "troya atları" və casus proqramlarını (Spyware – kompüterdə olan məlumatları əldə etmək üçün gizli şəkildə ona yüklənən proqram) tətbiq edərək kompüter təhlükəsizliyi sistemlərini sındırmaqla şəxsi, iqtisadi, siyasi və ya hərbi üstünlük əldə etmək məqsədilə icazəsiz informasiyanı (dövlət və hərbi sirlər) əldə etməkdir. Facebook və Twitter kimi sosial şəbəkələrin təhlükəli istifadəçilərinin davranışlarının təhlilini aparan və onlara zərbə endirən müəyyən proqramlar (Athena) da mövcuddur.

2. Təcavüz – internet səhifələrinə müdaxilə edərək onları dəyişdirmək və ora müəyyən təbliğat materialları yerləşdirməkdən, rəsmi kompüterlərdə olan gizli məlumatları oğurlamaq və onları dezinformasiyalarla əvəz etməkdən, dövlətin infrastrukturunun idarə olunduğu internet səhifələrini və ya kompüter sistemini sıradan çıxarmaqdan ibarətdir.

İnformasiya müharibəsi əsasən iki mərhələdən keçir:

1. Hərbi təcavüzə qədər olan mərhələ
2. Hərbi təcavüz ərəfəsində olan mərhələ

Hərbi təcavüzə qədər olan mərhələdə informasiya silahları vasitəsilə düşmən dövlətin maddi və mənəvi dayaqlarına zərbələr endirilir, onu ayaq üstə tutan bütün sosial, siyasi, iqtisadi və mədəni institutlarına qarşı hücumlar təşkil olunur, beynəlxalq aləmdə ölkənin imici aşağı salınır.

1. Hərbi təcavüzə qədər olan informasiya müharibəsi mərhələsi:

- ölkədə insan hüquq və azadlıqlarının məhv edilməsi, diktatura rejiminin hökm sürməsi, gender bərabərliyinin pozulması, dini radikalizmin baş qaldırması, dözümsüzlüyün artması, dini-etnik diskriminasiyaya yol verilməsi və digər bu kimi təbliğatlarla ölkənin beynəlxalq aləmdə neqativ imicini yaratmaq, həm də öz daxilində əhalinin iqtidara qarşı ayaqlanmasını təmin etmək;
- ölkədə etnik, dini və ideoloji separatçılığı qızışdırmaq, vətəndaş müharibəsi üçün zəmin hazırlamaq;
- iqtidar və müxalifət arasında gərginliyi pik həddə çatdırmaq, müxalifətə qarşı iqtidarın repressiyasına şərait yaratmaq;
- partiyalar, ictimai təşkilatlar arasında ədavət salmaq, onları qarşı-qarşıya gətirmək, münaqişələr yaratmaq və əhalinin dövlətçilik mövqeyində dayanan lider və təşkilatlara etimadsızlığını və şübhələrini formalaşdırmaq;
- ölkədə əhaliyə dövlət orqanları barədə dezinformasiyalar yaymaq, onların nüfuzunu əsassız ittihamlarla aşağı salmaq və hökumətin fəaliyyətini yarıtmaz hala gətirmək;
- ölkədə siyasi gərginlik və xaos yaratmaq üçün sosial şəbəkələr vasitəsilə ictimai rəyi formalaşdırıb onu yönəltmək, 5-ci kolonu yaradıb ona dəstək olmaq, təxribat törədən sosial qrupların təşkilini təmin etmək;
- ölkədə mitinqlərin, qiyamların, kütləvi etimadsızlığın olmasını təşkil etmək və onların genişlənməsinə dəstək olmaq;
- ölkədə gərgin durumu həll etməyə çalışanları neytrallaşdırmaq, qəbul edilən ciddi qərarların ləğvinə çalışmaq;
- İKT vasitəsilə seçkilərə müdaxilə etmək, onların strateji məqsədlər istiqamətində saxtalaşdırılmasına və arzu olunan namizədin qələbə çalmasına səy göstərmək [12, s. 134].

Biz, hərbi təcavüzə qədər olan informasiya müharibəsi nümunələrini postsovet məkanında baş verən son 20-30 il hadisələrində, "ərəb baharı"nda, Yuqoslaviya hadisələrində müşahidə etmişik. "Rəngli inqilablar" İKT vasitəsilə idarə olunur. Sosial şəbəkələr vasitəsilə ictimai şüur yönləndirilir. "Ərəb baharı" adı ilə tanınan sosial-siyasi proseslərin facebook, youtube texnologiyaları vasitəsilə idarə olunduğu barədə geniş araşdırmalar mövcuddur.

Facebook sosial şəbəkəsində süni şəkildə formalaşdırılan müthiş aqressiya sonradan öz əksini sosial qiyamlarda tapdı. Ölkələrin rəhbərləri vəziyyət nəzarətdən çıxdıqdan sonra interneti bağlamaq qərarına gəlmişlər. Lakin əksər ərəb ölkələrində meydana çıxan xaos imkan verirdi ki, müxalifət qruplarının arasında xarici kəşfiyyatın xüsusi təyinatlı qrupları da sərbəst şəkildə fəaliyyət göstərsinlər. Onlar tərəflər arasında gərginliyi artırmaq üçün müxtəlif metodlardan istifadə edirdilər. Bununla yanaşı, hadisə yerinə daxil olan KİV-lər (xüsusilə, CNN, Əl-Cəzirə) və onların əməkdaşları da hadisələrin gərgin həddə yetişməsi istiqamətində reportajlar hazırlayır və təxribatlar törədirdilər. Ənənəvi cəmiyyətdə yaşamaq istəməyən əksər gənclər də bu təxribatların fərqinə varmadan onlara asanlıqla uyurdular. Artıq belə bir durumda informasiya aqressorunun həmin ölkəyə ordu yeritməyə ehtiyacı yoxdur. O, informasiya silahları və texnologiyaları ilə

cəmiyyəti rahat şəkildə manipulyasiya etdiyi üçün həmin güclərin vasitəsilə öz məqsədinə nail olur [13].

Lakin hərbi təcavüzə qədər olan informasiya müharibəsi öz səmərəsini vermədikdə, ikinci mərhələyə, yəni, hərbi təcavüz ərəfəsində olan informasiya müharibəsi mərhələsinə keçid edir.

2. Hərbi təcavüz ərəfəsində olan informasiya müharibəsi mərhələsi:

ABŞ və NATO hər hansı bir ölkəyə hərbi təcavüz ərəfəsində informasiya müharibəsinin aşağıdakı alqoritmindən istifadə edir:

- Beynəlxalq dəstəyi əldə etmək üçün öz informasiya resursları vasitəsilə düşmən ölkənin və onun iqtidarının beynəlxalq imicinə ağır zərbə endirir, ona qarşı kollektiv hərbi təcavüz üçün süni hüquqi baza formalaşdırır. Məsələn, İraqa hücum etmək üçün Səddam Hüseynin gizli nüvə silahı hazırlaması barədə informasiyalar beynəlxalq KİV-də geniş yayılmışdı. Halbuki sonra məlum oldu ki, bütün bunlar hərbi təcavüz üçün bir bəhanədən başqa bir şey deyildi.

- Düşmən ölkənin rabitə infrastrukturunu sıradan çıxarmaq üçün sistemə kompüter virusları ötürülür.

- Kompüter məntiq bombaları vasitəsilə quru və hava nəqliyyat sisteminin, maliyyə və dövlət idarəetmə sistemlərinin elektron sistemini iflic vəziyyətinə salır və onların çökməsi ictimai təşvişə səbəb olur.

- Son dövrdə İKT-nin inkişafı ilə əlaqədar olaraq beynəlxalq münasibətlər sistemində "infosanksiya" termini meydana çıxmışdır. Bu özünü, hər hansı bir ölkəyə və ya şirkətə qarşı beynəlxalq cəza tədbirlərində büruzə verir. Məsələn, ABŞ-rı İraqda "səhrada tufan" hərbi əməliyyatları həyata keçirərkən İraqın bütün informasiya resurslarını blokadaya almış və onun informasiya sistemini iflic etmişdi. Eyni əməliyyatlar NATO-nun keçmiş Yuqoslaviyaya təcavüzü zamanı baş vermişdi.

- Ölkə daxilində gizli agentləri və ya kəşfiyyatçıları vasitəsilə enerji infrastrukturuna ağır zərbə endirir (terror) və nəticədə, enerji infrastrukturuna bağlı olan bütün həyat sahələri (banklar, media, televiziya, nazirliklər və s.) iflic vəziyyətinə düşür.

- Düşmən ölkənin ordusunun idarəetmə heyətinə informasiya resursları vasitəsilə dezinformasiyalar və yanlış əmrlər ötürülür. Bunlar, ordunun pərakəndə olmasına, idarədən çıxmasına və döyüş qabiliyyətini itirməsinə səbəb olur.

- Psixoloji əməliyyatlar üçün xüsusi təyinatlı hərbi təyyarələr vasitəsilə ölkənin dövlət televiziya kanallarının fəaliyyətini dayandırır və ora, ölkə rəhbərinin əvvəlcədən hazırlanmış saxta video çıxışlarını yerləşdirirlər. Bu saxta video çıxışların yayılmasının məqsədi, əhalinin siyasi liderə olan etimadını yox etməkdir.

- Düşmən ölkənin siyasi və hərbi elitasının parçalanması üçün onların xarici banklarda olan hesabları bağlanır və onların informasiya ünvanlarına hədələyici mesajlar göndərilir, anonim zənglərlə təslim olmağa dəvət edilir.

- Ölkədə 5-ci kalon və onun liderləri önə çıxır və siyasi hakimiyyəti ələ keçirməyə çalışır. Bir çox hallarda öz bank hesablarını və vəzifələrini itirmək istəməyən məmurlar onların tərəfinə keçir [14].

- Bütün bunlardan sonra ölkə ərazisinə hərbi güclərin yerləşdirilməsi və onların strateji obyektlərinin nəzarət altına alınması prosesi başlanır. Əksər hallarda, informasiya müharibəsinin təzyiqlərinə tab gətirə bilməyən hökumətlər təslim olur. Mövcud durumdan təşvişə düşən əhali də müqavimət göstərmək cəhdindən geri çəkilir. Çünki onların düşmənin ikinci mərhələdə başladacağı hərbi taktikalarına ve savaş texnologiyalarına qarşı dayanmaq gücü qalmır.

Nəticə

Göründüyü kimi, informasiya müharibəsi döyüşün taleyini həll edir. Buna hazır olmayan və müqavimət göstərə bilməyən ölkələrin hərbi qarşıdurmalara hazırlaşması mənasızdır. İnformasiya müharibəsi silahına qarşı durmadan, müdafiə olunmaq mümkün deyildir.

İstifadə olunmuş ədəbiyyat

1. Daniel Ventre. Information Warfare. Wiley - ISTE 2016.
2. Kettrie, Orde F. Lawfare: Law as a Weapon of War. Oxford University Press, 2016.
3. Johnson, Natalie. CIA Warns of Extensive Chinese Operation to Infiltrate American Institutions. Washington Free Beacon, March 7, 2018.
4. Maza, Cristina Iran Protests: Government Took Control of the Internet to Silence Dissent, Report Says. Newsweek, January 10, 2018.
5. Алексеев А.П., Алексеева И.Ю. Информационная война в информационном обществе. Вопросы философии, 2016, № 11.
6. Барабаш В. В. Государственная пропаганда и информационные войны. Учебное пособие / В.В. Барабаш, Г.А. Бордюгов, Е.А. Котеленец. М.: АИРО-XXI, 2015.
7. Дугин А.Г. Сетевые войны: угроза нового поколения. М. : Издательство «Евразийское движение», 2009.
8. Почепцов Г. Г. Информационные войны. Новый инструмент политики. М.: Алгоритм, 2015.
9. ***Раскин А.В.*** Некоторые философские аспекты информационной войны // Информационные войны, 2015, № 3 (35).
10. Чеботарева Н. И., Ковалева С. С. Информационная война как деструктивная форма стратегических социальных коммуникаций: технологии медиаманипуляции в СМИ // Актуальные проблемы науки и практики современного общества, 2016, № 1.
11. Юренков В. В. Информационная война как процесс манипулирования массовым сознанием и формирования парадигмально-ограниченного мышления // Миссия Конфессий, 2017, № 20.
12. Яницкий О. Н. Глобальное общество. Качественная модель осаждённого города: случай Алеппо (Сирия) // Социологическая наука и социальная практика, 2017, Т. 5, № 1.
13. Гавриков В. Отвечать за слова: как защитить общество от «фабрик фейков» 2018. URL: https://cont.ws/@contemplator/900836
14. Коротченко И. Технологии провокаций: новые тенденции информационной войны. https://cyberleninka.ru/article/n/ informatsionnye-voyny-mif-ili-realnost

Нураддин МЕХТИЕВ

ФАКТОР ИКТ В МЕЖДУНАРОДНЫХ ИНФОРМАЦИОННЫХ ВОЙНАХ

Резюме

Развитие ИКТ повлекло за собой большие перемены в мире. В последнее время международный терроризм и различного рода транснациональные организации используя возможности интернета расширили свой круг влияния. Для того, чтобы создать напряжение в отношениях между странами, они часто искусственным образом создают провокационный контент. В таких случаях создается положение, благоприятствующее недовольству между странами и нарушению определенных договоренностей. Так, посредством информационного оружия, используемого в информационных войнах, ставится под вопрос информационная безопасность государственных учреждений. В результате теряют свою актуальность традиционные методы обеспечения национального суверенитета и безопасности международных отношений.

Цель: выявить характер, суть, влияние на систему международных отношений и последствия международных информационных войн, и в то же время определить пути защиты от них.

Методология: в статье использованы методы анализа, синтеза, проведения аналогий, и сравнительного анализа.

Научная новизна: на данный момент в рамках традиционного международного права нет решений в отношении многих киберпреступлений. С этой точки зрения, ИКТ ставит нас перед необходимостью создания новых концепций международной политики и права.

Ключевые слова: глобальная информация, информационная инфраструктура, информационная система, ИКТ

Nuraddin MEHDIYEV

ICT AS A FACTOR IN INTERNATIONAL INFORMATION WARS

Abstract

Developments in ICT have resulted in major changes in the world. In the recent period, international terrorism and transnational organizations various in character have used the Internet to extend their sphere of influence. They often acted as provocateurs on the Internet to initiate confrontations between countries. In some circumstances, this creates friction between states and contravenes established agreements. The use of ICT as a weapon in the information wars threatens the security of state agencies using the virtual information space. This is because national governments cannot control that space. Consequently, traditional concepts of national sovereignty and the security of international relations lose their relevance.

Purpose: to identify the nature and essence of the international information wars, their impact on the system of international relations and the consequences, while at the same time determining protective measures.

Methodology: the paper makes use of analysis, synthesis, analogy and methods of comparative analysis.

Scientific novelty: many cybercrimes do not seem to fall for resolution within the framework of traditional international law. In this context, ICT necessitates the establishment of new international policy and new legal concepts.

Keywords: global information, information infrastructure, information system, ICT

Rəyçi: AMEA Fəlsəfə İnstitutunun aparıcı elmi işçisi, fəl. f.d. Rauf Məmmədov
Qəbul edilib: 14.04. 2019